

Katowice, 2024-10-01

ZAPYTANIE OFERTOWE

Na zakup licencji programu SIEM oraz świadczenie usług Security Operations Center

wraz z wsparciem technicznym

1. Zamawiający

„FARMACOL-Logistyka” Sp. z o.o.

Adres: ul. Szopienicka 77, 40-431 Katowice,

Sekretariat tel. +48 32 20 80 600, fax +48 32 20 22 497

NIP 5252409576, Regon 141107266

Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy Krajowego Rejestru Sądowego nr KRS 0000288521

Kapitał zakładowy w wysokości 481 621 600,00 zł w całości opłacony.

2. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

- zakup licencji na system SIEM
- świadczenie usługi Security Operations Center (dalej „SOC:”) z użyciem tego oprogramowania.

Zamawiający - „Farmacol-Logistyka” Sp. z o.o. podlega pod ustawę o krajowym systemie cyberbezpieczeństwa. W związku z tym świadczona usługa SOC oraz system SIEM musi spełniać minimalne wymagania regulacyjne – ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku oraz planowanych zmian w związku z koniecznością implementacji Dyrektywy NIS 2, w tym zagwarantowanie odpowiednich procesów monitorowania, detekcji i reakcji na incydenty bezpieczeństwa. Usługa musi spełniać wymagania związane z ochroną danych osobowych.

Usługa będzie świadczona dla Zamawiającego oraz podmiotów należących do Grupy Kapitałowej Farmacol które na moment zawarcia umowy lub w trakcie jej obowiązywania zostaną objęte obowiązkiem monitorowania bezpieczeństwa. Wykaz podmiotów z Grupy Kapitałowej Farmacol zawiera załącznik nr 7.

I. System SIEM

1. Przedłużenie/zakup subskrypcji na okres umowy, tj. w opcji pierwszej na 12 miesięcy, w opcji drugiej na 24 miesiące, licencji „Splunk Enterprise”, w wariantcie 50GB/dziennie, aktualna licencja ważna do dnia 31.12.2024r. Płatność za subskrypcję będzie realizowana przez Zamawiającego w okresach miesięcznych z dołu – łącznie z płatnością za usługi SOC. Dodatkowo istnieje możliwość zaproponowania oprogramowania SIEM Splunk – w formule licencji MSSP (Managed Security Service Provider) dla 50 GB dziennie (serwer licencyjny u Wykonawcy). W tym wypadku Wykonawca akceptuje możliwość przekroczenia licencji. System w tym przypadku nie może blokować/odrzucać logów/danych w przypadku przekroczenia dziennego limitu danych (w odniesieniu do wykorzystywanych w danym momencie licencji), jak również otrzymywanych zdarzeń na sekundę (EPS).
2. Przedstawienia informacji o cenie licencji Systemu QRadar w opcji pierwszej na 12 miesięcy oraz w opcji drugiej na 24 miesiące. Opłata za licencję oraz wdrożenie systemu powinna być zawarta w miesięcznej płatności. Wdrożenie QRadar do dnia 01 stycznia 2025.

II. Usługa Security Operations Center

1. Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego, przez okres w opcji pierwszej - 12 miesięcy, w opcji drugiej na 24 miesiące, następujących usług:
 - Świadczenie usług Security Operations Center monitorowania i reagowania na incydenty, ciągłe doskonalenie usługi oraz świadczenie usług dodatkowych, 3 linie wsparcia.
 - Monitorowanie z użyciem SIEM w trybie 24/7/365
 - Diagnostyka i naprawa błędów
 - Aktualizacje oprogramowania i patche
 - Przegląd systemu SIEM raz na 6 miesięcy
 - Ciągłe doskonalenie usługi – 5 nowych reguł rocznie, jeden przegląd SIEM rocznie.
 - Przygotowaniu wdrożenia (techniczne oraz dokumentacyjne: przegląd, przygotowanie do wdrożenia usługi)
 - Wdrożeniu outsource’owanych linii wsparcia,

- Implementacji komponentów technicznych outsourcingu SOC i systemu SIEM , w skrajnym przypadku dla SIEM Splunk implementacja może ograniczyć się do zmiany licencji (komunikacja, zapewnienie bezpieczeństwa komunikacji, zdalny dostęp do panelu),
 - Przeprowadzeniu szkolenia online z obsługi dostarczonego systemu (2-dniowe, zdalnie. łącznie 12 godzin zegarowych szkolenia – dla 10 osób) – dotyczy systemu Q Radar
 - Przygotowanie dokumentacji z wdrożenia (architektura, konfiguracja, scenariusze itp.)
 - Utrzymaniu wdrożonych komponentów systemu SOC,
2. Świadczenie usług wspierających SOC - pełnienie funkcji osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu Cyberbezpieczeństwa,

Rozmiar środowiska informatycznego (produkcyjne) Zamawiającego – stanowi załącznik nr 2.

3. Sposób przygotowania oferty

Oferta, która będzie załącznikiem do przyszłej umowy, powinna zawierać:

3.1 Dotyczy programu SIEM

- Informacje o cenie za licencję Splunk Enterprise na okres w opcji pierwszej na 12 oraz w opcji drugiej na 24 miesięcy, przy założeniu 50GB/dziennie. Dodatkowo istnieje możliwość złożenia informacji o cenie licencji proponowanego programu Splunk w formule licencji MSSP (Managed Security Service Provider) – dla 50 GB dziennie (serwer licencyjny u dostawcy).
- Opcjonalnie informacje o cenie za licencję programu - QRadar na okres w opcji pierwszej na 12 miesięcy oraz w opcji drugiej na 24 miesięcy, przy założeniu 50GB/dziennie,
- Opłata za licencję programu Q Radar będzie obejmowała – z uwagi na to, iż Zamawiający korzysta obecnie z systemu Splunk, przygotowanie planu wdrożenia, wdrożenie systemu w infrastrukturze Zamawiającego, migrację danych do nowego systemu oraz przygotowanie dokumentacji powykonawczej zgodnie z wymaganiami Zamawiającego. Wykonawca będzie zobowiązany do przeprowadzenia testów migracyjnych na środowisku testowym przed wdrożeniem do środowiska produkcyjnego.

3.2 Dotyczy usługi Security Operations Center

- Informację o cenie miesięcznej za usługę Security Operations Center.

3.3 Informacja o cenie za usługi dodatkowe w ramach SOC

- Kampania phishingowa 3 razy w roku skierowana do 400 wskazanych przez Zamawiającego pracowników.
- Świadczenie usług dodatkowych w wymiarze 16 godzin na miesiąc. Niewykorzystane godziny przechodzą na kolejne miesiące. Usługi obejmują między innymi: warsztaty, szkolenia, informatyka śledcza – analiza danych, zabezpieczenie dowodów, znalezienie źródeł incydentów, rekomendacje działań, analiza malware, kodu złośliwego, testy i skany podatności, doradztwo, konsulting itp.
- Informacja o cenie usług ponad wymiar 16 godzin na miesiąc - cena za 1 godzinę pracy.
- Informacja o cenie za pełnienie funkcji odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa.
- Informacja o usłudze oraz etapach realizacji:
 - Analiza przedwdrożeniowa, wdrożenie oraz uruchomienie podstawowej zdolności operacyjnej SOC w zakresie monitorowania oraz reagowania na incydenty.
 - Dostawa licencji, rozwój i wsparcie dla posiadanej konfiguracji systemu SIEM.
 - Optymalizacja usługi.
 - Implementacja scenariuszy bezpieczeństwa (przegląd i implementacja scenariuszy bezpieczeństwa posiadanych przez Farmacol (około 40) oraz do 5 nowych scenariuszy w każdym roku współpracy).
- Informacje o doświadczeniu z zakresie systemu Splunk lub QRadar podmiotu w zakresie usług bezpieczeństwa, szczególnie dla podmiotów podlegających pod ustawę o krajowym systemem cyberbezpieczeństwa w okresie ostatnich 3 latach, w formie zestawienia.
- Referencje/potwierdzenia realizacji usług SOC dla firm i innych podmiotów, w formule zbliżonej do treści zapytania ofertowego.
- Kopie certyfikatów PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 22301. Oferenci bez certyfikacji nie zostaną dopuszczeni do dalszego etapu postępowania.
- Potwierdzenie – w formie oświadczenia spełnienia wymagań dla podmiotu świadczącego usługi w zakresie bezpieczeństwa wynikające z Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa oraz przepisów wykonawczych w szczególności w zakresie

pomieszczeń: Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 roku w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa. – według załącznika nr 3

- Potwierdzenie spełnienia warunku – w formie oświadczenia o spełnienia warunku świadczeniu co najmniej 5 pełnowymiarowe usługi SOC o łącznej wartości minimum 1.500.000,00 zł rocznie według wzoru w załączniku nr 4.
- Potwierdzenie spełnienia warunku w formie oświadczenia - wykonawca zatrudnia co najmniej 10 osób – analityków bezpieczeństwa I, II i III linii wsparcia SOC, którzy posiadają specjalistyczną wiedzę. Na potwierdzenie stanu osobowego i kwalifikacji zostanie przedstawione zanonimizowane zestawienie zawierające informacje o poszczególnych osobach według wzoru w załączniku nr 5.
- Informacja o posiadanym ubezpieczeniu – kopia ważnej polisy odpowiedzialności cywilnej.
- Pełną nazwę Wykonawcy wraz z adresem i numerami telefonu, e-mail.
- Nazwiska osób upoważnionych ze strony Dostawcy do kontaktów z Zamawiającym.
- Szacunkowy harmonogram projektu.
- Oferta powinna zawierać czasy SLA dla podjęcia zgłoszenia incydentu, czas poinformowania Zamawiającego, czas dostarczenia rekomendacji.
- Oświadczenie, że Wykonawca utrzymuje monitoring oraz wsparcie telefoniczne i e-mailowe: 24/7/365 – według wzoru w załączniku nr 6.
- Wykonawca posiada i udostępnia w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF) – treść zostanie dołączona do oferty.
- Inne posiadane świadectwa bezpieczeństwa, osiągnięcia, certyfikaty, audyty itp. świadczące o dojrzałości Wykonawcy w zakresie bezpieczeństwa informacji oraz zapewnienia ciągłości działania świadczenia usług SOC.
- Obowiązuje język polski i czytelna forma oferty.
- Termin płatności: płatność za usługi miesięczna z 30 dniowym okresem płatności.
- Do oferty cenowej należy załączyć wzór umowy na realizację przedmiotu zamówienia w formie do edycji. Umowa powinna zawierać obowiązki dostawcy określone w NIS 2 (np. prawo do audytu, zachowanie ciągłości działania, powiadamiania o incydentach itp.)

- Oferta będzie stanowiła załącznik do umowy.

4. Tryb udzielenia zamówienia

Wybór najkorzystniejszej oferty.

5. Sposób ogłoszenia wyników

Zamawiający poinformuje drogą elektroniczną Oferenta o wyniku oceny Oferty (jak i zakwalifikowaniu się do dalszych etapów negocjacji).

6. Ocena ofert, informacje dodatkowe

- a) Zamawiającego nie obowiązuje ustawa o zamówieniach publicznych, lecz przepisy wewnętrzne.
- b) Zamawiający zakłada, iż wszystkie informacje udzielone przez Oferenta są prawdziwe. W przypadku wykrycia jakichkolwiek rozbieżności od stanu faktycznego, Zamawiający zastrzega sobie prawo natychmiastowego wykluczenia Oferenta.
- c) Zamawiający zastrzega sobie:
 - i. prawo do swobodnego wyboru Oferty,
 - ii. możliwość niedokonania wyboru Oferty,
 - iii. możliwość unieważnienia postępowania w każdym momencie jego trwania bez podania przyczyny.

W takim przypadku Oferentowi nie będą przysługiwały żadne roszczenia względem Zamawiającego.

- d) Koszty opracowania i dostarczenia Oferty oraz uczestnictwa w przetargu obciążają wyłącznie wykonawcę.
- e) Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji dotyczących przedstawionej Oferty z wybranymi Oferentami.
- f) Zamawiający zastrzega sobie prawo częściowego wyboru przedmiotu Oferty.
- g) Oferty oceniane będą pod m.in. kątem:
 - i. zgodności z zapytaniem ofertowym,
 - ii. warunków cenowych,
 - iii. terminu płatności.
- h) Zamawiający nie jest zobowiązany do wyboru Oferty z najniższą ceną.
- i) Zamawiający nie wyraża zgody na wyłączenie rękojmi z umowy.
- j) Treść zapytania oraz warunki i specyfikację techniczną proszę traktować jako poufne.

Klauzula informacyjna o przetwarzaniu danych osobowych dotycząca osób fizycznych i osób fizycznych prowadzących działalność gospodarczą, których dane osobowe są udostępniane Zamawiającemu w związku z prowadzonym postępowaniem. Na podstawie art. 13, 14 rozporządzenia unijnego o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informujemy, że: Administratorem danych osobowych pozyskanych w związku z prowadzonym postępowaniem jest Zamawiający. Kontakt do Inspektora: inspektor.odo@farmacol.com.pl. Dane osobowe będą przetwarzane w celu

prowadzenia postępowania, w celu kontaktu, w celu zawarcia i realizacji umowy, na podstawie przepisów prawa (art. 6 ust 1 lit. b, c, f RODO). Odbiorcami Pani/Pana danych osobowych będą podmioty mające dostęp na podstawie przepisów prawa oraz podmioty, z którymi zawarte są umowy powierzenia przetwarzania danych osobowych. Dane będą przetwarzane do czasu trwania postępowania o udzielenie zamówienia, realizacji umowy i wygaśnięcia roszczeń oraz upływu terminu określonego w odrębnych przepisach prawa dotyczących archiwizacji. Przysługuje prawo dostępu do danych osobowych, prawo do sprostowania, prawo żądania od administratora ograniczenia przetwarzania, prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
